PIANO DI FORMAZIONE NAZIONALE IN MATERIA DI *CYBER SECURITY, CYBER THREAT, PRIVACY*

SERVIZI FORMATIVI

Formazione specialistica, a catalogo e/o personalizzata

Tutti i prodotti formativi disponibili a catalogo sono caratterizzati secondo 4 dimensioni, utili per semplificare la fase di scelta da parte degli utenti destinatari:

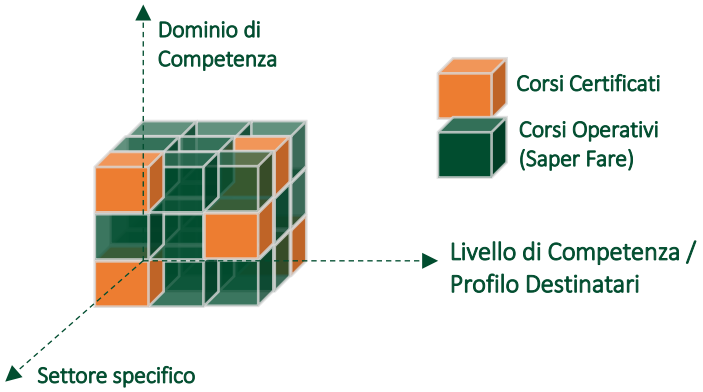
- Ambito / Dominio dei contenuti in relazione a Cybersecurity, Cyberthreat, Privacy e Data Protection:
  - Organizzativo/Gestionale
  - Giuridico-Normativo
  - Tecnologico
  - Relazionale

- Verticalizzazioni specifiche per Settore:
  - PA Centrale, Enti locali ed Aziende pubbliche ad alta criticità
    - A questo specifico riguardo *ad aprile 2016 è stato pubblicato lo standard italiano per le "Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni"*.
    - Tutte le iniziative formative destinate alle P.A. devono obbligatoriamente essere progettate in modo conforme a questo standard, nonché agli standard formativi di Cybersecurity previsti da NIST e promossi da ENISA
  - Settore Sanitario
  - Settore Finanziario / Bancario /Assicurativo
  - Energy
  - Infrastrutture Critiche in generale

- Livello di competenza / Profilo dei Destinatari
  - Livello Base (*Awareness*)
    - Consapevolezza delle minacce e dell'impatto potenziale dei rischi connessi ai comportamenti adottati da ciascun dipendente nel proprio ruolo
    - Consapevolezza delle responsabilità e delle buone pratiche sottese al proprio ruolo professionale
    - Conoscenza di policy e procedure
    - Comprensione della terminologia tecnica relativa ai principali modelli di Cyebrsecurity e Data Protection e agli eventi più rischiosi
  - Livello Gestionale (*Management*)
    - Conoscenza delle metodologie e dei framework organizzativi e tecnologici previsti dagli standard internazionali e nazionali in ambito IT Risk & Security Governance, Information Security Management e Data Protection, Privacy, Business Continuity, etc.
    - Comprensione delle dinamiche sottese ad un evento rischioso, capacità di individuazione e dimensionamento di impatti e soluzioni
  - Livello Tecnico (*Execution*)
    - Conoscenza dei metodi, delle tecniche e degli strumenti per poter implementare operativamente misure preventive e contromisure protettive sul campo
    - Conoscenza approfondita dei fenomeni rischiosi connessi alle piattaforme tecnologiche interne ed esterne al perimetro della propria organizzazione
    - Conoscenza approfondita delle procedure tecniche, documentali e comunicative per gestire sul campo la routine giornaliera e le occorrenze rischiose prevedibili ed imprevedibili

relativamente alla continuità operativa, alla prevenzione e alle attività di ripristino a fronte di emergenze

- Obiettivo formativo:
  - Formazione Certificata
    - Funzionale all'ottenimento di un titolo valido come riconoscimento ufficiale delle competenze acquisite (*es. Certificazioni ufficiali ISACA CISM, CSX, ISO 27001, ISO 22301, ISO 20000-1, DPO – Data Protection Officer, APMG COBIT5 for NIST Cybersecurity, etc.)*
  - Formazione Operativa (saper fare)
    - Orientata, tramite laboratori e soluzioni ad alta interattività, all'apprendimento delle tecniche, degli strumenti e delle procedure pratiche da applicare sul campo nelle attività day-by-day



Ambiti / Domini di contenuto

DOMINIO ORGANIZZATIVO - GESTIONALE	
Contesto	L'applicazione di adeguati interventi preventivi e protettivi in ambito Cybersecurity, Privacy e Data Protection richiede, alla base di tutto, la scelta e l'applicazione di specifici modelli organizzativi e gestionali di IT & RISK Governance, utili per la messa in opera di efficaci processi di Pianificazione, Gestione e Controllo (Plan-Do-Check-Act) Questi modelli organizzativi sono necessari anche per conformarsi ai requisiti e alle procedure di auditing da parte di Organizzazioni Capo-Gruppo, Organismi di controllo ed Enti di Certificazione, nonché per certificare le competenze dei professionisti chiamati ad implementare e a gestire i modelli stessi e/o a verificarne il corretto funzionamento.
Obiettivi Formativi	- Apprendimento delle competenze e degli strumenti necessari per l'applicazione all'interno dell'organizzazione Pubblica o Privata di uno o più Framework di IT Security Management, IT Risk Analysis & Governance, Data Protection & Privacy, Business Continuity & Disaster Recovery. - Formazione, ed eventuale certificazione ufficiale, delle figure professionali richieste per l'implementazione, la gestione e l'auditing dei modelli organizzativi e gestionali a cui si intende conformare l'organizzazione
Competenze Teoriche	Apprendimento degli standard internazionali, dei concetti chiave, dei principi abilitanti, dei processi e dei requisiti connessi ai modelli di Governance per gli ambiti scelti. A puro titolo di esempio: • NIST CYBERSECURITY FRAMEWORK • ISO 27001 – Information Security Management & Data Protection Systems • ISO 22301 – Business Continuity, Disaster Recovery & Incident Management systems • …
Abilità Pratiche	- Applicazione sul campo di tecniche di Risk Assessment e Business Impact Analysis, - Redazione di Piani strategici ed operativi, Budgeting, - Svolgimento di attività di verifica e monitoraggio e/o ispettive

PIANO DI FORMAZIONE NAZIONALE IN MATERIA DI *CYBER SECURITY, CYBER THREAT, PRIVACY*

	DOMINIO GIURIDICO - NORMATIVO
Contesto	FOCUS PRIVACY e DATA PROTECTION: • Il percorso formativo, declinato sia a livello nazionale sia europeo ed internazionale, prende in considerazione il nuovo regolamento europeo sulla Data Protection e gli altri atti normativi europei ed internazionali rilevanti in materia, il Codice in materia di protezione dati personali, i Pareri dell'Article 29 Data Protection Working Party, i Trattati internazionali sul trasferimento dei dati personali all'estero. Si analizzeranno alcuni dei principali provvedimenti del Garante per la protezione dei dati personali, delle Autorità giurisdizionali europee, internazionali ed italiane, anche attraverso percorsi pratici per la conformità alle normative di settore in ambito privacy nei confronti delle pubbliche amministrazioni e delle aziende, tenuto conto anche dei nuovi adempimenti relativi al regolamento europeo n. 679/2016, il quale sarà presto obbligatorio per tutti gli enti pubblici e nel settore privato. Il corso mira anche a consolidare il background accademico concreto ed esaustivo, necessario alle figure chiave della Privacy, che devono conoscere la disciplina nazionale e comunitaria a riguardo e, a seconda del settore in cui operano, potrebbe essere loro richiesto anche un bagaglio tecnico-informatico di buon livello. FOCUS INFORMATION & ASSET SECURITY • Il percorso formativo approfondisce i riferimenti legislativi attuali nazionali ed internazionali che, oltre alle tematiche di Privacy, devono essere presidiati per tutelare l'organizzazione Pubblica o Privata da rischi legali o di compliance connessi alla sicurezza delle informazioni, degli asset aziendali e degli stakeholders (es. Statuto dei Lavoratori, Dlgs. 231/2001, Aspetti contrattuali relativi a fornitori, clienti, terze parti, etc)
Obiettivi Formativi	FOCUS PRIVACY e DATA PROTECTION: • Formazione, ed eventuale certificazione ufficiale, delle figure professionali richieste obbligatoriamente dal nuovo regolamento europeo per la Privacy (DPO – Data Protection Officer) e delle altre figure necessarie per specifici ambiti settoriali (Es. Sanità, P.A., etc) e/o raccomandate dagli schemi di certificazione italiani ed internazionali (es. Manager/Responsabile Privacy interno; Specialista Privacy, Valutatore/Auditor Privacy) • Apprendimento delle competenze e degli strumenti necessari per la gestione delle problematiche legali e tecniche connesse alla conformità legale di settore in ambito privacy nei confronti delle pubbliche amministrazioni e delle aziende FOCUS INFORMATION & ASSET SECURITY • Apprendimento delle competenze e degli strumenti necessari per la gestione delle conformità alle norme ed agli standard internazionali di Sicurezza delle Informazioni e di Continuità Operativa
Competenze Teoriche	FOCUS PRIVACY e DATA PROTECTION • Analisi degli strumenti di tutela legale dell'interessato e della gestione degli adempimenti in ordine al riscontro da parte dei titolari del trattamento dei dati. Analisi della distribuzione dei compiti e delle responsabilità privacy all'interno dell'ente pubblico e delle società private. Studio delle metodologie di valutazione di impatto (c.d. Data Protection Impact Assessment, DPIA) FOCUS INFORMATION & ASSET SECURITY • Analisi degli strumenti di tutela dell'azienda pubblica / privata in relazione rischi legali o di compliance connessi alla sicurezza delle informazioni, degli asset aziendali e degli stakeholders (es. Statuto dei Lavoratori, Dlgs. 231/2001, Aspetti contrattuali relativi a fornitori, clienti, terze parti, etc)
Abilità Pratiche	FOCUS PRIVACY e DATA PROTECTION • Richieste di accesso privacy degli interessati, gestione dei riscontri degli interessati, gestione informative e comunicazioni alle authority e al management. Pianificazione dell'organizzazione della architettura privacy dell'ente pubblico e delle società private: mappature dei ruoli privacy, designazioni dei responsabili del trattamento dei dati e degli incaricati. Analisi degli scenari operativi in cui il responsabile della protezione dei dati personali svolge le proprie prestazioni. Applicazione delle metodologie di valutazione di impatto a scenari operativi. FOCUS INFORMATION & ASSET SECURITY • Richieste di accesso alle banche dati di pertinenza • Compilazione di check-list e stesura dei Modelli documentali e contrattuali necessari per l'espletamento delle formalità di audit e di business operation in modo conforme ai requisiti ed agli

PIANO DI FORMAZIONE NAZIONALE IN MATERIA DI *CYBER SECURITY, CYBER THREAT, PRIVACY*

	standard

DOMINIO TECNOLOGICO	
Contesto	Congiuntamente alla definizione dei modelli organizzativi e gestionali di riferimento ed all'applicazione dei requisiti di conformità giuridiche a norme e/o standard internazionali, è necessario proteggere fisicamente gli asset, le piattaforme, le infrastrutture e le reti aziendali, implementando le soluzioni tecnologiche ed applicative che consentano di individuare, contrastare e annientare o mitigare le minacce cibernetiche
Obiettivi Formativi	- Apprendimento, coerente con gli standard formativi previsti da NIST e promossi da ENISA, delle competenze tecniche, degli strumenti e delle tecniche utili a proteggere la propria organizzazione dai vari scenari d'attacco, riconoscendoli ed individuando tempestivamente le più adeguate contromisure in base alle specificità della propria realtà. -Particolare riferimento agli ambiti di Cyber-Sicurezza di Dati, Reti, Sistemi, Applicazioni e di Piattaforme tecnologiche specifiche operanti internamente ed esternamente al perimetro aziendale. - Fornire tutte le competenze specialistiche e le abilità pratiche utili per la gestione delle criticità tipiche di un CERT/CSIRT
Competenze Teoriche	Apprendimento delle competenze e degli strumenti necessari per presidiare e gestire sul campo tutte le fasi connesse alle attività di messa in opera e mantenimento di un'architettura di Cyber-sicurezza, e di identificazione, reazione e contrasto alle minacce: • Identify: Analisi, identificazione e valutazione di Assets, Minacce e Vulnerabilità sia su reti interne che esterne • Protect: Implementazione di controlli di Cybersecurity per proteggere un sistema o una piattaforma tecnologica specifica dalle minacce identificate • Detect: Rilevazione di Network e System incidents, indicatori di Evento e Compromissione, e dimensionamento del danno potenziale • Respond: Messa in atto di efficaci e tempestivi piani di risposta e mitigazione agli incidenti • Recover: Ripristino della continuità operativa a fronte di incidenti o eventi disastrosi, utilizzo di strumenti di Integrity Evaluation e Backup Dispersion, Approntamento tempestivo di servizi e task di backup secondario
Abilità pratiche	Sviluppo di capacità operative molto spinte tramite laboratori pratici e tutoraggio in aula ed online, anche su piattaforme tecnologiche specifiche: • Identify: Hardware / Software Identification -Advanced Scanning; Network Discovery Tools; Sensitive Information Discovery & Identification; Vulnerability Assessment Set-up, Configuration, Scan; Patch Upgrade & Configuration • Protect: Specific Cyber Controls & System Hardening; Collecting Event Data, Firewall Setup and Configuration; Verifying the Effectiveness of Controls, Microsoft Baseline Security Analyzer; Monitoring Controls , IDS Setup; Updating Cyber Security Controls, Personal Security Products; Patch Management Linux Users and Groups; Verifying Identities and Credentials; Cyber Security Procedures Standards • Detect: Analyze Network Traffic Using Monitors, Snort and Wireshark; Detect Malicious Activity, AntiVirus Detect; Assess Available Event Information, Analyze and Classify Malware; Baselines for Anomaly Detection, Windows Event Log Manipulation via Windows Event Viewer; Initial Attack Analysis, Host Data Integrity Baselining; Incident Escalation Reporting, Performing Network Packet Analysis; Change Implementation Escalation • Respond: Defined Response Plan Execution, Incident Detection and Identification; Network Isolation, Remove Trojan; Disable User Accounts; Blocking Traffic, Implement Single System Changes in Firewall; Incident Report, Create Custom Snort Rules • Recover: Disaster Recovery and BC Plans Patches and Updates based on Industry Best Practices; Cyber System Restoration, Data Backup and Recovery and Data Integrity Checks; Actualizing Data Backups and Recovery, Post Incident Service Restoration; Implementing Patches and Updates; Ensuring Data Integrity; Post-Incident Review

PIANO DI FORMAZIONE NAZIONALE IN MATERIA DI *CYBER SECURITY, CYBER THREAT, PRIVACY*

DOMINIO RELAZIONALE	
Contesto	Quando si concretizza una minaccia che non si riesce a contenere con gli strumenti e le risorse di monitoraggio e protezione preventiva, sia essa una violazione della Privacy o una compromissione di Informazioni e Asset strategici aziendali, oltre alle contromisure tecniche è fondamentale gestire il processo di comunicazione, rivolto all'interno e all'esterno dell'impresa privata o pubblica che sia tempestivo, completo, multidirezionale e incisivo. In particolare, questo flusso deve essere orientato in funzione del ruolo che, nella particolare contingenza, potranno assumere i principali "stakeholder" aziendali. Un'opportuna comunicazione, sia verso il personale ed il management, che verso l'esterno (media, clienti, fornitori, etc.) è fondamentale per evitare pericolosi effetti domino che rischiano di amplificare considerevolmente l'impatto del danno.
Obiettivi Formativi	Apprendimento delle competenze e degli strumenti necessari per la gestione delle criticità di sensibilizzazione e comunicazione interne ed esterne e dei flussi relazionali di crisi tra gli interlocutori dell'organizzazione durante tutto il ciclo di reazione alla crisi
Competenze Teoriche	Approfondimento delle Tecniche e delle metodologie per la gestione tempestiva ed efficace di tutte le fasi del processo di comunicazione in situazioni di crisi: Costituzione del gruppo di crisi, Stanziamento risorse, Definizione ed applicazione delle procedure di crisi (ruoli, informazioni, canali, destinatari, tempi) Monitoraggio degli effetti della comunicazione e analisi dei risultati.
Abilità Pratiche	Strumenti, tecniche e canali per la definizione, la gestione ed il monitoraggio efficace dei processi comunicativi interni ed esterni in fase di crisi

Modalità di erogazione

Le nostre soluzioni formative sono erogate in modalità differenti in base alla natura dei contenuti e alle esigenze di disponibilità dei partecipanti:

- Corsi in aula e/o online in modalità e-learning e/o Teleconferenza/Streaming
- Aule ad insegnamento frontale o Laboratori pratici ad alta interattività
- Soluzioni con contenuti standard a catalogo o *in house* / personalizzate *ad hoc*

Tipologia di formazionePercorsi di formazione ricorrente

- Seminari
- Workshop e corsi brevi
- Master universitari di primo e secondo livello
- Percorsi specializzanti
- Percorsi di formazione ricorrente

Network docenti e "Subject Matter Expert"

Ci avvaliamo di un **network selezionato** in continua evoluzione di esperti di settore:

- riconosciuti a livello nazionale ed internazionale,
- dotati delle principali certificazioni internazionali (es, ISACA, ISO / ACCREDIA, APMG, EXIN, etc)
- con esperienze accademiche e professionali sul campo distintive nei settori più critici rispetto agli ambiti della Cybersecurity e Privacy

Contatti: www.cresec.com - presidente@eCReSEC.uniroma2.it - segreteria@eCReSEC.uniroma2.it